The PGB Cryptosystem

Jussi Leiwo

Abstract. This paper introduces the PGB cryptosystem capable of withstanding extensive analysis by three letter acronyms. The strength of the proposed cryptosystem is based on the post-analysis activities of three letter acronyms and does not necessarily employ techniques that might prevent three letter agencies to carry out their tasks of preventing and investigating, say, organized email encryption.

1 Introduction

Three letter acronym (from herein referred to as an *acronym*) is vaguely defined in definition 1.

Definition 1. A three letter acronym is an ordered sequence $(\sigma_1\sigma_2\sigma_3)$ where each $\sigma_i \in \Sigma$ when $i \in \{1,2,3\}$ and Σ is the alphabet of a known language.

Examples of acronyms are ABC, DEF, and WH@. A three letter acronym is a fundamental construct in computer science in general, and areas of research such as telecommunications are driven into great difficulties due to the exhaustion of a three letter acronym base. In recent years, certain acronyms have proposed so called trapdoor cryptosystems allowing the acronyms to disclose the content of messages if they suspect such offenses as organized email encryption or Minnie laundry, i.e. washing in hot water images of well-known cartoon characters copyrighted by large multinational corporations in order to create psychedelic art. The disclosure procedure improves the privacy of Internet users by discouraging them from communicating any material over the insecure Internet.

In this paper, a new cryptosystem is proposed that can withstand even extensive cryptanalysis by acronyms. The algorithm is called Pretty Good Bull's hit (PGB) since after any attempt of cryptanalysis of a PGB-encrypted message, the cryptanalyst, often an acronym, can only speculate on what hit him/her/it. Hence, PGB provides hyperperfect secrecy, attempts to analyze messages encrypted with PGB have a negative impact on the analysis of messages encrypted with any other cryptosystem. This is due to the sociological phenomena related to the cryptanalysis as shall be studied later in this paper.

2 Assumptions

The PGB assumes the availability of two elements:

1. An acronym of form $P\alpha P$ where P is a symbol "P" in an alphabet, for example P, and α is any symbol in any alphabet so that when sandwiched

between the two Ps, such as P, as above, it forms a well-defined acronym, for example POP, or PPP. Under certain conditions the above rule can be relaxed, and for example sequences such as DES, can be valid acronyms of form $P\alpha P$.

2. A high number of internally consistent pseudo-random sequences of cryptographic literature of adequate length. Internal consistency refers to the property of being internally consistent, that is on align with principles of cryptographic literature, such as low text-to-equation –ratio, unintuitive reasoning, and ignorance of real world constraints. However, the sequences must not be external consistent, i.e. be relevant to the cryptographic community and on align with previously published externally consistent results. Such sequences are easy to find from both published and unpublished manuscripts.

3 PGB Encryption and decryption

Let m be a message to be PGB-encrypted with E_k that is a well-formed acronym of form $P\alpha P$ where k is an instance of a symbol "k", and r be a pseudo-random sequence of adequate length. To improve the applicability of the technique, E_k can be any string representing the name of an encryption function. Adequate length is defined as the number of symbols on r being high enough. Let symbol $|$ refer to the concatenation operation that concatenates two strings by concatenating them.

Now A (being the abbreviation of sender "Sender", so the name of the sender, that is "Sender", is called "A") wants to send message m to B (being the abbreviation of the name of a receiver "Receiver"). A simply calculates the ciphertext c as follows:

$$c = E_k(r|m) \tag{1}$$

and sends c to B. B then reverses the operation by calculating

$$(r, m) = K_k(c) \tag{2}$$

and discards r carefully, preventing any eye contact with it. The avoidance of eye contact is the key to the capacity of PGB encryption to withstand any cryptanalysis and to provide hyperperfect secrecy as evaluated in the following.

4 Security evaluation

The security is based on the well known "exam marking" phenomena, sometimes also known as "assignment marking" phenomena. This refers to the excessive work factor required for the recovery of tasks such as marking exams or assignments at the end of a semester. Often, the amount of work required to "get the facts right again" after reading a high number of exams or assignments is comparable to the study of 4 to 5 text books of the topic of exam or assignment. Confusion and diffusion are well known security design principles, yet author suspects not exactly this kind of confusion is meant.

However, novel application of confusion is the key to the security of PGB. It is assumed that the acronym analyzing c has the capability of disclosing the pair (r, m) from c. However, after (r, m) has been recovered from c, there is a task of filtering out random string r. No better algorithm than RIAS (Read it all sugar[1]) is known for that. Application of RIAS, though, is likely to cause symptoms of a severe exam marking phenomena in the reader, hence improving the strength of cryptosystem by three means:

1. Causing resources of an acronym to be directed to re-educational activities, hence reducing the resources available for other activities.
2. Causing a negative cumulation of knowledge in the acronym's knowledge base of cryptanalysis and therefore strengthening also other cryptosystems.
3. Repetitive subjection of a cryptanalyst to PGB is likely to have severe negative side effects on the analyst, hence improving the "nutty professor" value of the analyst and, therefore, paving the way towards an academic career, hence promoting academic research.

5 Conclusions

A new cryptosystem has been proposed that achieves hyperperfect secrecy without requiring the length of an encryption key to be more than, say, 40 bits, well enough to protect one's diary from systematic analysis attempts by any little sister or brother, yet balanced with the need of acronyms of reading all messages transmitted over the Internet to prevent severe criminal activities such as use of offensive language in personal communication. The reference implementation is currently being developed and voluntary cryptanalysts are called to aid in the practical evaluation of the proposed scheme.

This article was processed using the LaTeX macro package with LLNCS style

[1] sometimes replaced with a slightly more explicit expression